WIRELESS COMMUNICATION ENABLED METER AND NETWORK

The subject matter of this application is related to the subject matter of copending U.S. Patent application serial numbers 60/179,041, 60/179,046 and 09/621,965, entitled "Wireless Communication Enabled Meter and Network," "Wireless Communication Enabled Meter and Network," and "System and Method for a Virtual Network Operations Center," respectively, each having the same inventors as this application, each being assigned or under obligation of assignment to the same assignee as this application and each incorporated herein by reference.

Field of the Invention

This invention relates to a meter that is enabled for wireless communication. More specifically, this invention relates to a meter, such as a utility meter, that is enabled for wireless communication. The invention also relates to a self-configuring, wireless network that enables data capture at a plurality of metering sites and wireless transmission of the captured data from the plurality of metering sites to one or more collection points.

Background of the Invention

Remote communication with meters is known, for example, for home load control and for usage monitoring. Commands for home load control are typically transmitted over telephone lines or power lines. Communicating via power lines or telephone lines is

slow and subject to physical disruption. Moreover, communicating via power lines or telephone lines presents the possibility of spurious signals, cross-talk, and other interference. One-way or two-way radios are also sometimes used. Both are expensive and two-way radios also require a license.

With regard to usage monitoring, on the other hand, utility meters are normally read by a person visiting the meter. In recent years, a number of schemes have been contemplated to accumulate usage data, as by counting wheel revolutions per unit time and storing such information as a preliminary necessity for actually automatically transmitting such information upon command of a remote central station.

Local area networks that interconnect via cables are also known. These networks are expensive to install and somewhat intrusive in that cables must be run to physically interconnect the various nodes in the network. Moreover, networks that are interconnected with cables are subject to physical disruption of the cables.

Recently, wireless networks have been developed. These networks can be used to collect information from, and to disseminate information to individual nodes of the network. For example, conventional wireless networks generally operate using a loop configuration in which each node in the network is interconnected and communicates only with two neighboring nodes. Information and/or commands are passed from node to node around the loop until they arrive at a master node. The master node is used to communicate information that is gathered to a central station, or to accept and distribute information received from a central station throughout the network.

Conventional wireless networks, however, have limitations as well. For example, because conventional wireless networks generally have a loop configuration, when one node is disabled, the integrity of the entire network is affected. Moreover, if the master node of such a conventional network is disabled, the network becomes isolated.

These and other drawbacks exist with current systems.

Summary of the Invention

An object of the invention is to overcome these and other drawbacks in existing systems.

Another object of the invention is to provide a meter that is enabled for wireless communication.

Another object of the invention is to provide a self-configuring wireless network.

According to one embodiment, a wireless communication enabled meter is disclosed. A meter enabled for wireless communication comprises a metering device, a wireless communication system and an interface between the two. The metering device is a standard programmable metering device that can measure usage data and control usage. The wireless communication system is enabled for wireless communication using, *e.g.*, the Bluetooth™ protocol. The interface facilitates communication between the metering device and the communication system so that meter data can be read with a wireless network using, *e.g.*, the Bluetooth™ protocol.

According to another embodiment, a self-configuring wireless network is disclosed. The wireless network comprises a number of virtual nodes ("vnodes"), and

one or more virtual gates ("VGATES"). Vnodes are operative to form *ad hoc* piconet connections. Vnodes can comprise a variety of devices. Data traveling through the network is passed from one or more ad hoc piconets to one or more of the vnodes or an uploading point, *e.g.*, a VGATE. If a vnode is not connected to a piconet, or if its connection to a piconet has been disturbed, the vnode executes a self-configuration routine to connect itself with another piconet. This self configuration process is based on a set of rules. The one or more VGATES comprise computer network gateways enabled for communication.

Other features and advantages of the present invention will be apparent to one of ordinary skill in the art upon reviewing the detailed description of the present invention.

Brief Description of the Drawings

Fig. 1 is a schematic diagram of a wireless communication enabled meter.

Fig. 2 is a schematic depiction of a self-configuring wireless network according to another embodiment of the present invention.

Fig. 3 is a schematic depiction of a self-configuring wireless network according to another embodiment of the present invention.

Fig. 4 is a schematic depiction of a self-configuring wireless network according to another embodiment of the present invention.

Fig. 5 is a schematic diagram showing a self-configuration process according to one embodiment of the present invention.

Fig. 6 is a schematic diagram showing a self-configuration process according to one embodiment of the present invention.

Fig. 7 is a schematic diagram showing a self-configuration process according to one embodiment of the present invention.

Fig. 8 is a schematic diagram showing a self-configuration process according to one embodiment of the present invention.

Fig. 9 is a schematic representation of the system for an embodiment of the invention.

Fig. 10 is a black box representation of an embodiment of the invention.

Fig. 11 is a black box representation of another embodiment of the invention.

Fig. 12 is a schematic representation of components of the system for an embodiment of the invention.

Fig. 13A is a schematic of an embodiment of the VNOC architecture for an embodiment of the invention.

Fig. 13B is a schematic of an embodiment of network architecture.

Fig. 14 is a black box representation of an embodiment of the invention employing redundant architecture.

Detailed Description of the Preferred Embodiments

Figure 1 schematically depicts a meter 1 that is enabled for wireless communication. Meter 1 may comprise metering device 2, interface 3 and wireless

communication transceiver 4. In operation, metering device 2 may communicate with wireless communication transceiver 4 via interface 3. Wireless communication transceiver 4, in turn, may communicate with other wireless communication enabled devices, for example, other meters 1 or a central station. Wireless communication transceiver 4 may be operative to transmit data to and receive data from other meters 1 equipped with transceivers 4.

Metering device 2 operates to measure and regulate the usage of some utility, *e.g.*, natural gas, electricity, or water. According to one embodiment, metering device 2 comprises any known metering device capable of producing an analog or digital output signal indicative of utility usage. In another embodiment, metering device 2 comprises a metering device capable of accepting an analog or digital input signal and for monitoring and controlling utility usage. For example, metering device 2 is operative to monitor utility usage. Utility usage data is useful in the electrical industry, for example, to control future generation in order to avoid over generation or under generation of electricity. According to another example, metering device 2 is operative to monitor power quality. The power factor of electrical power, for example, may vary with usage. Metering device 2 can monitor this variance. In turn, household devices that are also enabled for wireless communication can be controlled to change the load and correct the power factor. According to one particular embodiment, metering device 2 comprises the Altimus™ produced and sold by Landis & Gyr Utilities Services, Inc.

Interface 3 facilitates communication between meter 1 and wireless communication transceiver 4. According to one embodiment, interface 3 receives digital

signals from wireless communication transceiver 4 and in response produces digital control signals for meter 1 and/or metering device 2. Interface 3 also receives digital signals from metering device 2 and outputs digital signals suitably formatted for transmission through wireless communication transceiver 4. According to one embodiment, interface 3 comprises a software module. According to another embodiment, interface 3 is implemented in firmware or hardware. Conventional interfaces may be employed as interface 3 in some embodiments of the invention.

Wireless communication transceiver 4 operates to wirelessly transmit and receive data and other information. According to one embodiment, wireless communication transceiver 4 is operative to receive control information and to transmit usage data accumulated by metering device 2. According to one particular embodiment, wireless communication transceiver 4 comprises a Bluetooth™ communication chip. Bluetooth™ is explained in detail in *Bluetooth* [*sic*] *Document Page* (visited Nov. 15, 1999), <http://www.bluetooth.com/document/default.asp?page=overview> *(Bluetooth™ Specification)*, herein incorporated by reference. According to another embodiment, wireless communication transceiver 4 comprises a transceiver operative to communicate using another suitable wireless transmission protocol, such as an ultrawide band protocol.

Briefly, Bluetooth™ is a wireless communication protocol operating in the unlicensed ISM band at 2.4 GHz that enables wireless communication of data and voice. The Bluetooth™ system operates through a collection of short-range radio links, built into 9 x 9 mm microchips, *i.e.*, Bluetooth™ chips. The short-range radio links enable ad hoc groupings of connected devices away from fixed network infrastructures.

Bluetooth™ uses an acknowledgment and frequency hopping scheme to make network links robust. Specifically, Bluetooth™ radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet of data. The Bluetooth™ radio uses faster hopping and shorter packets than other systems operating in the same frequency band. Short packages and fast hopping make the Bluetooth™ system robust, *e.g.*, by limiting the impact of domestic and professional microwave ovens and other potential sources of interference.

Bluetooth™ uses Forward Error Correction (FEC) to limit the impact of random noise on long-distance links. The encoding is optimized for an uncoordinated environment. A frequency hop transceiver is applied to combat interference and fading. A shaped, binary FM modulation is applied to minimize transceiver complexity. The gross data rate is 1Mb/s. A Time-Division Duplex scheme is used for full-duplex transmission.

The Bluetooth™ baseband protocol is a combination of circuit and packet switching. Slots can be reserved for synchronous data packets. Each data packet is transmitted in a different hop frequency. A packet nominally covers a single slot, but can be extended to cover up to five slots. Bluetooth™ supports an asynchronous data channel, up to three simultaneous synchronous voice channels, or a channel which simultaneously supports asynchronous data and synchronous voice. Each voice channel supports 64 kb/s synchronous (voice) link. The asynchronous channel can support an asymmetric link of maximally 721 kb/s in either direction while permitting 57.6 kb/s in the return direction, or a 432.6 kb/s symmetric link.

Using Bluetooth™, meter 1 transmits data to, for example, a central collection point via other Bluetooth™ enabled devices (*e.g.*,other Bluetooth™ enabled meters) forming an *ad hoc* network. Moreover, meter 1 receives data from a central controller via other Bluetooth™ enabled devices through a similar type of *ad hoc* network.

According to another embodiment of the present invention, a self-configuring (*i.e., ad hoc*) wireless network is disclosed. A self-configuring wireless network may be advantageously formed using the wireless communication enabled meters disclosed in conjunction with Figure 1. A self-configuring wireless network will be explained in more detail in connection with Figure 2.

Figure 2 schematically depicts an embodiment of a self-configuring wireless network 20 according to the present invention. Network 20 may comprise a number of piconets 21 and a VGATE 22. Each piconet 21 may comprise a plurality of individually addressable vnodes 23 that are wirelessly linked together. For example, in a Bluetooth™ system, a piconet may comprise a plurality of Bluetooth™ units sharing a common channel.

According to one embodiment, network 20 comprises a number of layers. The layers may include (1) A layer for configuring the network. This layer is used to establish and support connections between the various vnodes 23 to VGATE 22. (2) A layer for upstream communications, *i.e.*, communications from vnodes 23 to VGATE 22. And, (3) A layer for downstream communications, i.e., communications from a central computer network to vnodes 23 through VGATE 22.

These layers may be in addition to the layers that may be present in a particular wireless communication transport agent that may be used. According to one particular embodiment, these three layers are established using the proprietary Telemetry Technologies Communications Protocol™ ("TTCOM™") established by Telemetry Technologies.

TTCOM™ is a communications protocol used for inter-device communications for Telemetry Technologies™ products. TTCOM™ does not explicitly specify the transport media of communication between devices. The physical and data layer capabilities may be device specific and may be modified to suit different hardware needs. For example, TTCOM™ may be implemented on a Serial RS232 link, a SPI bus connection, a parallel interface, a radio network, a network connection (TCP/IP), the Internet or any other means used to exchange octets reliably between two devices.

The TTCOM™ may be peer-to-peer, i.e. all devices are equal and can query each other. All communications may be in a half-duplex Poll Response (client/server) format, i.e. each query from a client device may generate a response from the server device. Only one request from any client to any server may be outstanding at anytime. TTCOM™ may be implemented as a hierarchical master/slave protocol at the application level, if desired.

According to another embodiment, Bluetooth™ is used as the wireless communication transport agent.

In operation, each vnode 23 receives command or other data through *ad hoc* network 20, one instance of which is shown in Figure 2. For example, command data may be transmitted through VGATE 22 to piconets 21. The data is passed through the

various piconets 21 until it arrives at the piconet 21 which contains the destination vnode 23. Network 20 can also be used to collect information from vnodes 23. For example, as will be explained in more detail below, vnodes 23 may comprise devices that are designed to collect data. Collected data may be passed through the various piconets 21 until arriving at VGATE 22. From VGATE 22, collected data may be passed to a private or public computer network, such as system 26. Alternatively, data arriving at VGATE 22 may be passed to VNOC 25 where it can be uploaded to, for example, system 26, via a variety of wireless communication methods as will be explained in more detail below.

Vnodes 23 comprise individually addressable entities enabled for wireless communication. Vnodes 23 can be originators, recipients or routers of data. According to one embodiment, each vnode 23 has its own IP address so that commands can be sent to and data can be collected from individual vnodes through VGATE 22. As will be explained in more detail below, VGATE 22 may be a computer gateway that enables communications between public or private computer networks 26 and network 20. According to one embodiment, vnodes 23 maintain a routing table with information about two separate groups of entities. The first group comprises vnodes 23 that are potential gateways for this vnode. Typically, one of the vnodes in this list has an acknowledged active route to a gateway such as VGATE 22. According to one embodiment, this route is stored in non-volatile memory so that a vnode may attempt to establish a connection with VGATE 22 without going through the self-configuration process described below. The second group comprises vnodes 23 that have a confirmed route to a gateway using

this vnode as an intermediate hop. The concept of hops to a gateway is explained in more detail below in conjunction with the self-configuring process.

According to one embodiment, a vnode 23 comprises a device enabled for wireless communication using the Bluetooth™ protocol. According to this embodiment, vnode 23 may communicate with any other Bluetooth™ enabled device. For example, in one particular embodiment, a vnode 24 comprises a meter enabled for wireless communication using the Bluetooth™ protocol as explained in conjunction with Figure 1. According to other embodiments, a vnode 23 may comprise a vending machine, an alarm system or electric distribution equipment.

As explained in the *Bluetooth™ Specification*, Bluetooth™ uses a number of multiplexed communication channels to communicate between devices. Each channel comprises a slightly different transmission frequency. According to the embodiment of network 20 shown in Figure 2 in which each of vnodes 24 comprises a Bluetooth™ enabled device, two of the Bluetooth™ communication channels may be reserved for data passing between piconets 21. One channel can be used for upstream communication and the second channel can be used for downstream communication. In this way, upstream communication and downstream communication may be handled simultaneously. When data is passed between two piconets 21 in one direction, the vnode 23 of the piconet 21 that is engaged in the communication can determine if there is data to be passed in the other direction and may pass any such data off to the vnode 23 from which it received data. The use of other wireless communication protocols is possible.

Piconets 21 are operative to relay data to and from a central collection point through VGATE 22 using the wireless communication capabilities of vnodes 23 explained above. Piconets 21 may comprise, for example, *ad hoc* wireless networks of up to eight vnodes 23. Each vnode 23 in a piconet 21 at any instant of time knows about the existence of the other vnodes 23 that are connected to the piconet 21. In particular, each vnode 23 may know the identities (*e.g.*, the IP address) of the other vnodes 23 and the type of data at the other vnodes 23 that are connected to piconet 21. This facilitates the above-described passing of data to and from the individual vnodes 23 and among piconets 21. More specifically, communications between piconets 21 need only take place through one of the vnodes 23 in a piconet 21 to one of the vnodes 23 in another piconet 21. According to another embodiment, any other suitable number of vnodes may be used to form piconets 21 given the limits of the communication protocol being used and the hardware.

As schematically depicted in Figure 2, each of the rows of vnodes 23 may form a piconet 21. Data passing through the network 20 "hops" from one piconet 21 to another piconet 21 via wireless connections as shown in Fig. 2. These wireless connections are depicted at a particular instant in time and may change as piconets 21 are reconfigured. Data travels until it reaches the appropriate destination which may be VGATE 22 for data traveling upstream or one or more of vnodes 23 (or another Bluetooth™ enabled device) for data traveling downstream.

Because data sharing takes place among the various vnodes 23 of a piconet 21, network 20 of the present invention may also include security measures to protect the data

of each vnode 23. According to one embodiment, the IP address of each vnode 23 comprises an encryption key that is used by each particular vnode to decode incoming data. The same encryption scheme may be used to encode all outgoing data from any vnode 23 as well. In this way, although each vnode 23 of a piconet 21 has access to the data for each of the other vnodes 24 of a piconet 21, the data is in encrypted form. Thus, the data is unreadable to the other vnodes 23of the piconet 21.

Returning to Figure 2, VGATE 22 operates to manage network 20. As manager of network 20, VGATE 22 may comprise both a communication gateway and an administrator for network 20. As a communication gateway, VGATE 22 comprises a gateway that enables wireless network 20 to communicate with a private computer network or a public computer network such as the Internet. According to one embodiment, VGATE 22 comprises a standard computer gateway enabled for Bluetooth™ communication. According to this embodiment, VGATE 22 may communicate with network 20 wirelessly using the Bluetooth™ protocol. Further, VGATE 22 may communicate with a public or private computer network using conventional means (wired communication). In operation, VGATE 22 can receive information, such as control data, from a private computer network and retransmit that information to any of vnodes 23 through network 20 using the Bluetooth™ protocol. Further, VGATE 22 can receive data from any of vnodes 23 via network 20 using the Bluetooth™ protocol and then retransmit that information through a private computer network. Other embodiments of VGATE 22 are possible.

According to another embodiment, VGATE 22 may be enabled to communicate using a number of separate wireless devices. Thus, the number of vnodes 23 that any VGATE 22 may act as a gateway for is increased. According to one embodiment, VGATE 22 is equipped with two or more Bluetooth™ chips and its capacity is at least doubled.

VGATE 22 may also act as an administrator for network 22. Specifically, VGATE 22 may comprise intelligence about the configuration of network 20. According to one embodiment, VGATE 22 comprises an intelligence module that contains the geographic location of all vnodes 23 within a certain distance of VIGATE 22 and a list of all vnodes 23 that are presently communicating with VGATE 22. This is useful for example for locating specific vnodes 23, for example, for service purposes. For example, assume each vnode 23 represents a utility meter 21 in a residential neighborhood. If one of the meters 21 is not functioning properly, a repair person can determine the location of the vnode 23 from VGATE 22. Alternatively, if a repair person is driving through the neighborhood, that person can connect to network 20 using the self configuring process (explained below) as a vnode 23 would. Once connected, the repair person can use VGATE 22 to locate the non-functional vnode 23.

Although only a single VGATE 22 is shown in Figure 2, network 20 may comprise a number of VGATES 22. Because VGATE 22 acts as a communication hub for network 20, the number of VGATES 22 in any network 20 will depend upon the bandwidth available. As described above, when data is passed through each piconet 21, it is determined whether additional data is to be passed. Thus, when data is passed through

each piconet 21, additional content may be added to the data being passed. Therefore, to help ensure that the bandwidth limitations of the communication protocol are not exceeded, a sufficient number of VGATES 22 are deployed through a network 20.

In another embodiment, shown in Figure 3, at least two networks 31-37 may be daisy chained together to form a network cluster, such as network cluster 39. For example, each network 31-38 may represent a separate building. Thus, each building network 31-38 may be connected to another building network through individual vnodes 30a-30h. In this embodiment, the network cluster may be connected to one VGATE 22.

Thus, a first network 34 may be connected to a first VGATE 22 and a second network 33 may be connected to the first network by connecting a first vnode 30a in the first network to a second vnode 30b in the second network. Additional networks 31, 32 may be added to the network cluster where each network 31-34 communicates with the first VGATE 22 through the network cluster connections (i.e. network 31 communicates to VGATE 22 through networks 32, 33 and 34 while network 34 communicates directly with VGATE 22).

In another embodiment, networks 31-38 need not create a daisy chain path to communicate to a VGATE 22 through the geographically nearest network. For example, a network 38 may communicate to a VGATE 22 through a network 35 although network 35 is not the geographically nearest network to network 38.

In a further embodiment, the direct path formed from the VGATE 22 to a vnode 30a-h or network 31-38 need not be from the VGATE 22 to the nearest vnode 30a-h or

network 31-38. For example, network 37 may form a direct path to VGATE 22 through vnode 30g although network 37 is not the geographically nearest network to VGATE 22.

Referring to Figure 2, system 26 may comprise a central controller. VGATE 22 may facilitate connection to a central control controller 26. According to one embodiment, where vnodes 23 comprise utility meters 21, a utility company may read the meters 21 remotely and control utility usage by communicating with network 20 through VGATE 22. The central controller in this embodiment may be the computer network of the utility company. According to another embodiment, vnodes 23 may comprise vending machines and a management company can monitor stock in the vending machines by communicating with the machines through network 20 using VGATE 22. In this embodiment, the central controller may be the computer system for the management company. In another embodiment, VGATE 22 may facilitate communication between a monitoring company and a network of alarm systems when vnodes 23 are residential or commercial alarm systems. In still another embodiment, VGATE 22 may facilitate communication between an electric generation company and its distribution equipment that are enabled to communicate using a wireless communication protocol.

Returning to Figure 2, network 20 may also connect with other devices. Figure 2 depicts network 20 connecting with VNOC 25 and other devices 24 that are enabled for wireless communication. Each is explained in more detail below.

As discussed above, VGATE 22 facilitates communication between network 20 and other public or private computer networks using, *e.g.*, conventional wired networking. In contrast, VNOC 25 comprises a virtual network operation center.

According to one embodiment, VNOC 25 comprises a universal communication adapter that is enabled to transmit and receive using a variety of communication protocols and media. VNOC 25 is capable of communicating using RF, cellular, microwave, satellite and other communication protocol. According to one embodiment, VNOC 25 communicates with VGATE 22 in order to facilitate communication between network 20 and other non-wired networks. For example, VNOC 25 can receive command data for network 20 via satellite communication and retransmit the command data to VGATE 22 for distribution to vnodes 23. According to one particular embodiment, VNOC 25 comprises the VNOC system sold by Telemetry Technologies, Inc.

According to another embodiment, VNOC 25 may communicate directly with vnodes 23. In this embodiment, VNOC 25 is enabled for communication using the Bluetooth™ communication protocol. For example, VNOC 25 may receive command data for any of vnodes 23 via any of its enabled communication protocols. VNOC 25 may then retransmit the command data to the appropriate vnode using the Bluetooth™ protocol. Conversely, VNOC 25 may receive collected data from one or more of vnodes 23 via network 20 using the Bluetooth™ protocol and then retransmit the collected data to another location using an appropriate one of its enabled communication protocols. Accordingly, VNOC 25 enables communication with devices forming part of network 20 using a number of different communication protocol or media. VNOC 25 is especially useful for networks 20 installed in remote or rural areas where hard wire connections are uneconomical. A detailed description of VNOC 25 is provided in conjunction with Figures 7-12 below.

Network 20 may also connect with other devices 24. These other devices 24 are similar to vnodes 23 in that they are enabled for wireless communication. According to one embodiment, these other devices 24 are dissimilar from vnodes 23 in that they do not have the capability to connect as members of piconets 21. These other devices 24 are able to communicate through network 20 by connecting to a vnode 23 as shown in Figure 2. According to one embodiment, these other devices may comprise devices that are enabled to communicate using the Bluetooth™ protocol. In a particular embodiment, these other devices may comprise thermostats, pool pumps, and other household devices (refrigerators, washers, dryers, electronics) that are enabled to communicate using the Bluetooth™ protocol. According to another embodiment, these other devices are enabled to form piconets 21 and act as vnodes 23.

According to one embodiment, network 20 is formed by deploying utility meters that are enabled for wireless communication throughout a neighborhood. The utility meters act as vnodes 23 to establish the infrastructure of network 20. Once network 20 is deployed, it may be used to control other household devices such as pool pumps, thermostats and appliances (other devices 24) that are also enabled for wireless communication. According to one particular embodiment, Bluetooth™ enabled meters are deployed throughout a neighborhood to form the infrastructure for network 20. Network 20 is then used to communicate with other Bluetooth™ enabled devices in the neighborhood.

In another embodiment, shown in Figure 4, the network 20 may be a wide area network to optimize communication in rural areas. Network 20 may include piconets

21a, 21z. As shown, piconet 21z is a distance D from its geographically nearest piconet 21a in network 20. High gain, directional antennas 41-42 may be used to provide a line of sight point to point connection between vnode 23a of piconet 21a and vnode 23z of piconet 21z. Antennas 41-42 form fixed links, and boost decibel gain and power in the network 20. Use of antennas 41-42 to form connections between vnodes 23a, 23z allows the range from the Bluetooth™ equipment to be increased to at least approximately 17 miles.

As discussed in the background, conventional wired networks suffer from drawbacks such as physical disruption. One advantage of the embodiments of wireless network 20 discussed above is that it does not depend on wired connections. Another advantage of wireless network 20 discussed above is its self configuring nature. Therefore, if there is an interruption in the network structure, the network can reconfigure itself. More specifically, each of vnodes 23 is programmed to periodically poll the other vnodes 23 of its piconet 21 to determine that piconet 21 is still intact. If a vnode 23 determines through its regular polling routine that it is no longer connected to a piconet 21, it performs a self-configuring cycle in which it looks for another piconet 21 to join.

The self-configuring cycle of a vnode 23 within network 20 is based on a number of rules. One example of such a rule is that a vnode 23 in search of a piconet 21 will only connect with a piconet 21 that is in search of a vnode 23. As another example, each vnode 23 within network 20 may be programmed with a maximum of hops that it can use in order to reach a communication point (VGATE 22 or VNOC 25). The maximum number of hops for any vnode 23 is preferably based on geography. That is, when a

vnode 23 is deployed, it may be programmed with information concerning the geographic location of the closest uploading point. Therefore, by rule, when a vnode 23 goes through its polling routine, it can be instructed not to connect to any piconet 21 if the connection would result in a maximum number of hops to a VGATE 22 or VNOC 25 equal to, or greater than, its maximum number of hops. Moreover, a vnode 23 may be programmed to connect to a piconet 21 that has the smallest number of hops to an uploading point. As still another example of a self-configuring rule, when a vnode 23 is looking for a piconet 21 to connect with, it may be programmed to connect with piconets 21 that have connections to two or more other piconets 21. In this way, a measure of redundancy can be built into self-configuring network 20. Other rules are possible and are within the skill of the ordinary artisan.

According to another embodiment, any particular vnode 23 may connect with multiple networks 20 at any given instant in time. As explained above, according to one embodiment, self-configuring network 20 utilizes two communication channels available within the Bluetooth™ communication protocol for upstream and downstream communication. According to another embodiment, however, multiplexing is used in conjunction with those two communication channels allowing each vnode 23 to be part of a number of different networks 20 at the same time.

With reference to Figures 3-6, an example of self configuration of network 20 will now be given. For the example shown, it will be assumed that all vnodes 23 in network 20 are UNCONFIGURED (represented by white circles). The circles in Figures 5-8 represent either individual vnodes 23 or piconets 21. As shown in Figure 5, in the first

step when vnodes 23 bootup, they wait a pseudo-random amount of time (to avoid network flooding after a global power down) before broadcasting a request for a VGATE. The vnodes then wait for a valid response from other vnodes to setup their routes. If no valid response is received, the request message is again broadcast after a pseudo-random delay. This process is repeated till a valid response is received from another vnode 23. During this time if the vnode 23 receives a message from a VGATE it stops broadcasting the request message and stores the transport-agents parameters for access to the VGATE 22 in its routing table. In the example shown, as vnodes a-m are broadcasting requests for a VGATE, VGATE v may be broadcasting a message identifying itself as a VGATE.

As shown in Figure 6, in the next step of network configuration, vnodes j, k, l and m successfully receive a message being periodically broadcasted by VGATE 22. These vnodes 23 update their routing tables and stop broadcasting the request message. These vnodes are now configured with a zero metric. The metric indicates that these vnodes 23 have a direct link to VGATE 22.

Vnodes a-i may continue broadcasting request messages after pseudo-random delays. VGATE v may continue broadcasting a message identifying itself as a VGATE.

Now, some of the vnodes 23 that have a route to the VGATE 22 configured, receive a request messages from unconfigured vnodes 23 and choose to respond with a message indicating their availability as a path to a VGATE v. The metric in their response is set to 1. For example, vnodes j-m may respond to vnodes e-i. Vnodes 23 which receive this response message can choose to update their routing table with the new path. On the other hand, if the metric, usage or transport-agent provided parameter

(*e.g.* radio signal strength) is unacceptable the vnodes can simply discard the response and wait for responses from other vnodes. For example, vnode e receives a response from vnode k providing a route to VGATE v, but the metric is too high. This is illustrated in Figure 7. In the example shown, vnodes f-i have multiple routes, based on metrics. The dotted lines represent discarded routes. The primary gateways may be sent acknowledgements.

This process continues until all vnodes are configured. The completion of the configuration process is shown in Figure 8. It should be noted that each of the vnodes shown in Figures 5-8 may represent individual vnodes 23 or the vnodes pictured may actually represent individual piconets 21. It should also be noted that any vnode a-m, not only the geographically nearest vnodes, may connect directly to VGATE v. For example vnode d may be directly connected to VGATE v.

When undergoing this self-configuration process, vnodes establish connections with each other. According to one embodiment, these connections are established between two vnodes using a three step handshake. For example, assume a connection is being established between vnode X (desiring a route) and vnode Y (providing a route).

Step 1 vnode X broadcasts request for route to VGATE.

Step 2 vnode X possibly receives multiple replies from various vnodes. It chooses vnode Y to be its Gateway (based on metric and transport-agent parameters).

Step 3 vnode X acknowledges to vnode Y confirming that Y is now the Gateway for X.

Once this route has been established, X and Y are able to exchange messages and depending on the transport agent periodically check each other for messages to be exchanged. In case there is an error (a vnode fails, or communications fails) it is then the responsibility of vnode X to find another route by sending out a request. A vnode can explicitly send a message to a VGATE requesting a deletion of a route by sending a message.

Data propagation through network 20 will now be explained in more detail. Data propagates through network 20 in individual packets. According to one embodiment, packets to be sent to VGATE 22 have a destination of zero. The vnode 23 that originates the packet sends the packet through its gateway path vnode to vnode until the packet reaches VGATE 22. Each vnode 23 processing the packet decrements the address of the packet. If the address reaches zero, the packet is discarded. This is a mechanism to avoid looping packets in circular paths. As the packets pass through each vnode 23, an entry is made in the packet to record the route of the packet. The route is stored in VGATE 22 and provides a path for data directed from VGATE 22 to the vnode 23.

A packet exchange between nodes can be done in an acknowledge or non-acknowledge mode. Sending data in an acknowledge mode helps ensure that the packet is delivered to its intended recipient. According to one embodiment, acknowledgements are piggybacked on other data traveling through network 20 to reduce network traffic.

If a packet delivery fails, e.g., due to a vnode 23 failure, the vnode 23 delivering the packet starts a new search for a path to VGATE 22 by sending out a request, just as if

it was a new vnode 23. Additionally, it should be noted that a VGATE 22 can delete a route at any time, *e.g.*, to preempt excess traffic problems. VGATE 22 typically does not terminate any packet delivery until receiving acknowledgements from all vnodes. A vnode may search for a path to a VGATE 22 at any time, even if it is configured. This enables a vnode 23 to search for a more efficient path and thus enables the network to fine tune itself. As stated above, vnodes 23 may store a preferred route in non-volatile storage and attempt to establish this route directly without searching for a link.

As explained above, network 20 comprises a three layer network on top of an existing transport agent such as Bluetooth ™. According to another embodiment, one or more additional layers may be added. According to one particular embodiment, a layer may be added to form networks between various VGATES 22. This layer would enable, among other things, the capacity of network 20 to be increased.

VNOC 25 will now be explained in conjunction with Figures 9-14. Typically, the VNOC system is intended to provide seamless service for the customer. For example, the following description of one embodiment of the VNOC system is provided with reference to a remote water meter controller. The water metering customer has a remotely located water supply implementing a remotely controllable water metering valve. The customer desires to control the metering valve, monitor its status, and collect other data pertaining to the valve (*e.g.*, daily throughput, average water temperature, or other data). If a particular circumstance should occur (*e.g.*, the water flow drops below a predetermined level), the water valve meter sends a signal in whichever format the remote controller implements (*e.g.*, cellular, wireline, Internet, or other format). The VNOC system

provides the interface to receive data from the remote valve in that format and records the occurrence of an incoming event. The VNOC translates the incoming event into the outgoing event format (or formats) pre-selected by the customer. If the incoming event is one that the customer designated as requiring notification, the selected notification report is sent to the customer over the appropriate customer interface (*e.g.*, facsimile, pager, email, *etc.*).

If desired, the customer can take appropriate action through a customer interface. For example, the customer may send a command to the remote valve (*e.g.*, open until the flow rate reaches a certain level). Such a command may be sent through the customer interface (*e.g.*, inputting a code through a telephone tone/number sequence, inputting a command into a web browser, or other method). The VNOC receives the command from the customer and records another incoming event. The VNOC then translates the customer incoming event into the proper network outgoing event format and sends the command to the remote valve for implementation.

Figure 9 is a schematic representation of VNOC system 25 communicating between various customer facing interfaces and network facing interfaces. Customer interfaces may comprise any suitable interface over which a customer may communicate with the monitoring or control device. For example, customer interfaces may comprise computer interfaces such as a web browser, an electronic mail (email) interface, or a custom Internet protocol (IP) application. Customer interfaces may also comprise telephone interfaces such as a modem, an IVR, a facsimile machine, and a pager. Customer interfaces may also comprise custom interfaces such as a control and

monitoring host, for example, a supervisory control and data acquisition ("SCADA") host. Other customer interfaces are possible.

The various customer interfaces communicate with VNOC 25 over an appropriate network. For example, computer related customer interfaces (*e.g.*, web browser, email interface, or custom IP application) communicate with VNOC 25 over a computer network 31 such as the Internet or a local intranet. Other computer networks (WANs, LANs, *etc.*) are possible. Similarly, telephone related customer interfaces (*e.g.*, modem, IVR, fax machine, or pager) communicate with VNOC 25 over a telephone network 32 and custom devices communicate with VNOC 25 over a suitable custom network 33 (*e.g.*, X.25, VSAT, SCADA, wireless, etc.).

The various network facing interfaces communicate with VNOC 25 over an appropriate network. The communication may be accomplished over typical wire line, wireless, or other network. For example, VNOC 25 communicates with network facing interfaces using Bluetooth™, cellular, satellite, interconnected computer (*i.e.*, the Internet), or other networks. VNOC 25 communicates over networks with various third party network services. For example, VNOC 25 may communicate with third party network services such as Bluetooth™ 34, MicroBurst 35, the Internet 36, Mobitex 37, OrbComm 38, GSM 39, Cellemetry 40 and other future networks 41. The various third party network services may communicate with various I/O devices. The I/O devices enable monitoring and control of various systems. Monitoring and control may be implemented by any suitable input or output. For example, input and output may comprise digital, analog, AMR, or other signal formats.

Developer interfaces 42 may also communicate with VNOC 25. The developer interfaces 42 may be used by customers or others to enable other desired programs and applications. For example, developer tools such as Java/Bean, ODBC/SQL, OPC, LIB/DLL, ActiveX, COM, DCOM, ORB, and others, may be used to adapt telemetry applications in communication with VNOC 25.

As shown in Figure 10, the various customer and network interfaces communicate through the transmission of events through VNOC 25. Inbound events may originate at the customer interface (*e.g.*, inbound event 200), or the network interface (*e.g.*, inbound event 206). These inbound events are processed into corresponding outbound events (*e.g.*, outbound events 204 and 202). As noted above, events correspond to occurrences (or the lack of an occurrence) pre-selected for customer monitoring. In other words, the events are situations for which the customer desires to be notified. Thus, events may comprise physical occurrences (*e.g.*, a meter records a certain value, a pre-selected inventory item is shipped, *etc.*) or other less tangible occurrences (*e.g.*, a pre-selected stock price is reached, a certain sales volume is reached, a particular email message is received, a particular time period has expired, a dat file has been transferred, a point-to-point message is received, *etc.*).

For certain events a customer may desire notification. Such notification may comprise a report sent to the customer in a pre-selected format (or formats for multiple reports). Other events may trigger other services. For example, some events may be set up to cause an automatic response from VNOC 25 (*e.g.*, if a predetermined meter safety reading is exceeded, then automatically shut down the I/O device). Other services are

possible. Reports and services associated with an event may be collectively considered as transactions. As shown in Figure 11, transactions may be inbound 300 or outbound 305. Such a configuration enables the reporting and processing of event data using a publish/subscribe paradigm. Reports and services triggered by an event may be handled as a single transaction.

Figure 12 is a schematic representation of internal structure of VNOC 25. VNOC manager 100 manages communication between customer interfaces and network interfaces. Event manager 102 enables the management of events passing through VNOC 25. For example, events such as incharge, onset to offload, dependencies, concurrence, and others may be managed by event manager 102. Publication/subscription manager 104 enables the management of customer subscription to, and network publication of events. Configuration manager 106 manages the configuration of various VNOC 25 components by enabling, for example, customer specification of interfaces, protocols, services and other criteria. Security manager 108 enables management of various security measures implemented in the VNOC system. For example, security measures such as access rights, revocation, auditing, and other security functions may be managed by security manager 108. Error and recovery management manager 110 enables the management of error detection and recovery from errors. For example, error and recovery functions such as, notification, logging, recovery, backups, secondary paths, and other functions may be managed by error and recovery manager 110. Replication redundancy manager 112 enables various replication features. For example, redundancies between machines and locations, hot failure switchovers, persistence, rollovers, and other

replication features may be managed by replication redundancy manager 112. Customer billing module 114 enables, among other things, the tracking and billing of customer usage. For example, customer billing module 114 may manage the tracking of the level of usage, accumulation of bills, charges to third party interfaces, and other billing functions. Audit and log module 116 enables auditing and logging of various information. For example, location, levels, access, presentation, historical presence, and other information may be managed by audit and log module 116. Event naming module 118 manages the naming of events and may communicate with event database 120. For example, using an extensible markup language (XML) style event naming.

Figures 13A and 13B represent an embodiment of the VNOC architecture. As shown in Figure 13A, the VNOC architecture compares with the open systems interconnection (OSI) reference model network architecture. The OSI reference model 550 provides for various layers of network architecture (as shown in Figure 13B). For example, the OSI layers may include a physical layer 71, a data link layer 72, a network layer 73, a transport layer 74, a session layer 75, a presentation layer 76 and an application layer 77. In an embodiment of the VNOC, physical layer 71 may comprise the various Ethernet, serial port, RF, modem, wireless, and other, physical connections as supported by the I/O device. Transport layer 74, network layer 73 and data link layer 72 may comprise the various protocols that make up the network and customer interfaces (*e.g.*, WinSock, TCP/IP, IPX/SPX, UDP, SLIP/PPP, and other proprietary protocols). The session layer 75, presentation layer 76 and application layer 77 comprise the various VNOC processes described herein.

The VNOC architecture enables various features which provide for increased flexibility. For example, the VNOC system allows uniform representation of event data collected from a variety of I/O points, hand held devices, computers and networks. In addition, the reporting and receipt verification of events can be provided in any available customer protocol and interface. The symmetric design also provides for the customer to be an I/O point and provide an incoming event into VNOC 25. The VNOC architecture allows one user to connect to multiple I/O points, hand held devices or computers (one-to-many), multiple users to connect to one I/O point, hand held device or computer (many-to-one) and multiple users to connect to multiple I/O points, hand held devices or computers (many-to-many).

Additional features of the VNOC exist. For example, users are provided with simple and flexible interfaces, which they are accustomed to and, over which they can interact with their I/O points for feedback and control purposes. Furthermore, the VNOC allows users to query the system to retrieve desired data. Additionally, the VNOC provides the ability to summarize data at user specified level of detail and for user specified periods of time.

Figure 14 represents a schematic of an embodiment of the VNOC system. As shown, such an embodiment enables high availability of the VNOC by providing multi-redundant systems (*e.g.*, VNOC 25A, VNOC 25B, and VNOC 25C). Other multi-redundant features (*e.g.*, multi-redundant servers, connections, and geographic locations) also ensure reliability and availability of the VNOC system.

The VNOC remote monitoring system can be combined with other related technologies to provide more sophisticated notification and/or data collection systems. For example, two way pager notification can be employed as an add-on to the system. Also, integrated voice response can be employed in the system to enable the system to confirm that a particular notification has, in fact, been received by the proper personnel. Other features, such as fax on demand and web presence, can be employed to provide periodic information updates via fax or internet. This feature is particularly useful when a data collection center is collecting data from a plurality of remote monitoring systems (such as network 20 shown in Figure 2) and compiling the data for analysis purposes. A variety of other technologies can be easily interfaced with the VNOC system to allow customization of each product to the user's needs. For instance, the system can be adapted for security monitoring and reporting applications to use, for example, the Mobitex PCS network for the transmission of video capture of intrusions or status of monitored area.

The systems explained in conjunction with Figures 1-4 and 9-14 can be employed in a variety of different applications which are suited for remote monitoring. For example, in addition to monitoring devices such as meters and wireless networks as discussed in Figures 1-4, the system of Figures 1-4 and 9-14may be employed to monitor devices such as vending machines, drop boxes, sewer and water treatment facilities, flood control systems, railroad systems, waste management systems, environmental management systems, oil and gas pipelines, traffic systems, electric, gas and water utility systems, and medical alert systems. The system of Figures 1-4 and 9-14may also be

employed as part of a quality management system. Other applications will be apparent to persons skilled in the art.

The wireless communication capabilities discussed in Figures 1-4 and 9-14of the present invention may be employed for the remote monitoring of vending machines such as food or beverage dispensing machines. For example, a remote monitoring system can be installed in or near a vending machine and connected to appropriate sensors to monitor such characteristics as power status, product inventory, available monetary change status and a variety of general dispensing functions to ensure that the vending machine is operating properly at all times. Sensors may be any conventional system for acquiring the type of data which is to be monitored. For example, many vending machines include electronic circuitry which acquires some or all of the data required by the remote monitoring system of the present invention. In such a case, it is only necessary to connect the electronic circuitry of the vending machine with the input/output and/or expansion ports of an appropriate interface and to include a wireless communication system such as a Bluetooth™ wireless system.

A main power module can be connected to the available power source for the vending machine for operation. When a remote monitoring system detects a problem with the vending machine, data indicating the type of problem, such as a malfunction or depletion of inventory, can be communicated to the appropriate source for action. This allows service personnel to be dispatched promptly when they are required. Moreover, with appropriate equipment, information about the cause of the problem can be communicated to service personnel to provide them with an idea of the situation that

needs to be addressed. Thus, the vending machine can be promptly serviced, when required, and unnecessary visits to the vending machine can be eliminated.

The present invention may also be employed as part of a waste management system to monitor such things as the need for pick-up at a particular dumpster, the truck count at a dumpster and/or to determine whether a particular truck is full and needs to unload. This could be done by interfacing conventional sensors at dumpster sites with a wireless communication system such as the Bluetooth™ system. In this manner, trucks can be more efficiently deployed to make pick-ups where needed and to avoid unnecessary pick ups. This may permit a reduction in the number of trucks required to service a particular area and/or allow alterations of the size or placement of dumpsters to efficiently accommodate the need for same.

The present invention is also applicable to monitor various aspects of utilities including gas, electric and water utilities. For example, the meters in individual households can be replaced by, or upgraded with meters that are enabled for wireless communication such as the meters discussed in conjunction with Figure 1. These meters provide remote reporting of utility usage to a data collection center. Further, water, gas and electricity distribution systems can be monitored using the present invention for both failure detection and to collect data useful to determine efficient ways to operate such distribution systems. Additionally, a variety of different key pieces of equipment employed by utilities can be monitored using the system of the present invention.

Other embodiments and uses of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein.